

Information Security Officer Meeting

January 14, 2010

Meeting Agenda



- Welcome
- Short Subjects:
 - ◆ Open Source Software - IT Policy Letter 10-01
 - ◆ Draft Geocode ITPL
 - ◆ Draft Social Media ITPL and Standard
 - ◆ Draft Telework ITPL and Standard
 - ◆ Enterprise Risk Assessment Grant (\$2.35 million)
 - ◆ DNSSEC Grant (\$1.35 million)
- Legislative Update
- Incident Management
 - ◆ OIS Reporting
 - ◆ CHP Computer Crime Investigations Unit
- Q & A and Clsoing

Welcome

SIMM Form Updates



SIMM Form Changes:

- Name Change from OISPP to OIS
- Other minor clarification changes
- SIMM70A (Agency Designation Letter) and
- SIMM70C (Agency Risk Management and Privacy Program Compliance Certification)
- Forms due January 31, 2010

Open Source Software IT Policy Letter 10-01

[excerpt from published final]



PURPOSE:

The purpose of this Information Technology Policy Letter (ITPL) is to formally establish the use of Open Source Software (OSS) in California state government as an acceptable practice

POLICY:

The OCIO permits the use of OSS. Consistent with other software, use of OSS is subject to the software management licensing and security practices included in the SAM, Sections 4846, 4846.1, 5310–Item 2 and Item 5 Subsection (f), and 5345.1.

Geocode ITPL and Standard

[excerpt from draft]



PURPOSE:

This policy letter establishes a policy that requires the use of geocodes for all stored street address data elements.

POLICY:

It is the policy of the State of California to require Geocodes are for all addresses maintained in state data systems.

Social Media ITPL and Standard

[excerpt from draft]



PURPOSE:

The purpose of this Information Technology Policy Letter (ITPL) is to announce social media security standards and practices.

POLICY:

... shall comply with the agency management requirements and the Social Media Standards as described in the State Information Management Manual Section 85 A.

Social Media ITPL and Standard

[excerpt from draft]



State Information Management Manual Section 85 A.

- Conduct a formal risk assessment
- Formally document management's acceptance, mitigation, and handling of the risks involved
- Disable Internet access to Social Media websites ... until authorized by agency management ...
- Users shall connect to, and exchange information with, only those Social Media websites that have been authorized by agency management ...

Telework ITPL and Standard

[excerpt from draft]



PURPOSE:

The purpose of this Information Technology Policy Letter (ITPL) is to establish the Telework Security Standards in the Statewide Information Management Manual (SIMM) Section 85B as requirements for state government agencies and departments.

POLICY:

Agency heads shall ensure that only authorized users who have been trained regarding their roles and responsibilities, security risks, and the requirements included in the referenced standards, be permitted to telework.

Telework ITPL and Standard

[excerpt from draft]



State Information Management Manual Section 85 B.

- ... agency heads shall ensure that managers, supervisors, and telework users receive security training ..
- Only authorize telework user access to resources which are necessary to carry out the telework arrangement safely and securely. ... Telework user accounts shall, as a rule, be set up to have limited privileges.
- Telework user accounts shall require two-factor authentication, except when using a Web-based connection, such as Outlook Web Access (OWA) or other similar interface.

Telework ITPL and Standard

[excerpt from draft]



State Information Management Manual Section 85 B. (continued)

- Agency IT Administrators shall log and monitor all telework access. Log files shall capture sufficient detail to allow a virtual reconstruction of the end-to-end network session.
- Telework users shall not connect personally-owned information assets to the state IT infrastructure at the network-level unless an approved written exception applies and is implemented in accordance with the additional standards which apply to use of personally-owned information assets herein.

Telework ITPL and Standard

[excerpt from draft]



State Information Management Manual Section 85 B. (continued)

- In the rare situation where it is not possible to use state-owned information assets to establish a network-level connection in order to telework, the agency head, in consultation with the agency Chief Information Officer (CIO) and Information Security Officer (ISO), will consider the increased risk to the state, the agency, and the telework user posed by the telework user connecting to state IT infrastructure with personally-owned information assets.
- If the agency Head chooses to accept the risk ... the exception and risk approval shall be in writing and maintained for at least two years ...

Telework ITPL and Standard

[excerpt from draft]



State Information Management Manual Section 85 B. (continued)

- Personal networks can be wired or wireless. ... The telework user shall take the following precautions before connecting to a state agency IT infrastructure from an information asset attached to a wired personal network: ...
- The telework user shall take the following precautions before connecting to state agency IT infrastructure from an information asset attached to a wireless personal network: ...

State Enterprise Cyber Security Risk Program – Grant B



- Nineteen (19) month project with specific deliverables.
- ... leverage NIST 800-30, modified to meet California's needs, as a standard to better identify and manage risks across the enterprise ...
- The risk assessment process will integrate a series of interviews, system level vulnerability assessments, documentation reviews and analysis to identify known risks and measure the effectiveness of current controls to mitigate known risks.
- Includes funding for hardware, software, training, and consulting.

Secure ca.gov Domain Name System – Grant E



- Thirty three (33) month project to begin ASAP
- ... align the State of California with the Federal .gov domain security objectives and provide a trail of authentication and data integrity throughout the city/agency .ca.gov domain zones for trustworthy and reliable e-government communications and operations.
- DNSSEC's major objective is to provide the ability to validate the authenticity and integrity of DNS messages in such a way that tampering with the DNS information anywhere in the DNS system can be detected. This is the kind of protection that the ca.gov DNS servers require as Critical Infrastructure.

Legislative Update

Incident Management

Topics



- Roles and Responsibilities
- Required Reporting Process
- Reporting Stats
- CHP-Computer Crime Investigations Unit

Roles and Responsibilities



- Office of Information Security
- California Highway Patrol
 - Emergency Notification and Tactical Alert Center (ENTAC)
 - Computer Crime Investigations Unit (CCIU)
 - Counterterrorism & Threat Awareness Section (CTTA) for the Safety Service Program (SSP)
- Others (e.g., CalOHII, DGS, BSA)
- Reporting Organization

What's an Incident?



“An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.” Source: FIPS 200

Specific criteria for state agency reporting is found in state policy – State Administrative Manual section 5350.2

Overview of Reporting Process



1. Call ENTAC @ (916) 657-8287 to report a suspected or actual incident.
2. Await further contact from or initiate contact with:
CCIU: (916) 874-9300
OIS: (916) 445-5239
CTTA: (916) 843-3240
3. Prepare written report(s):
SIMM 65C – OIS
STD. 99 – CHP
STD. 152 – DGS
Others (e.g., CalOHII, BSA)

Partnership to Automate Reporting Process Underway

- OIS and CHP are partnering with CalEMA to automate the incident reporting process
- New system will:
 - Eliminate redundant manual reporting processes
 - Improve management reporting capabilities
 - Enhance visibility and gauge of state's security posture

Observations/Trends

Data Breaches

- One or more of the notice triggering personal data elements identified in Civil Code Section 1798.29
- Regardless of the type of media involved
- Includes inadvertent loss or disclosure, and suspected and actual theft and misuse
- Continue to rank number one
- Handling errors continue to be the primary cause

Observations/Trends



Asset Loss & Theft

- Continue to rank number two
- Carelessness and insufficient asset management controls continue to be primary cause
- Little to no accountability (e.g., cost recovery)

Observations/Trends



Website Compromises

- Continue to rank number three
- Poor coding practices continue to be primary cause
- Other causes
 - Weak passwords
 - Failure to decommission old servers/applications no longer maintained or in use

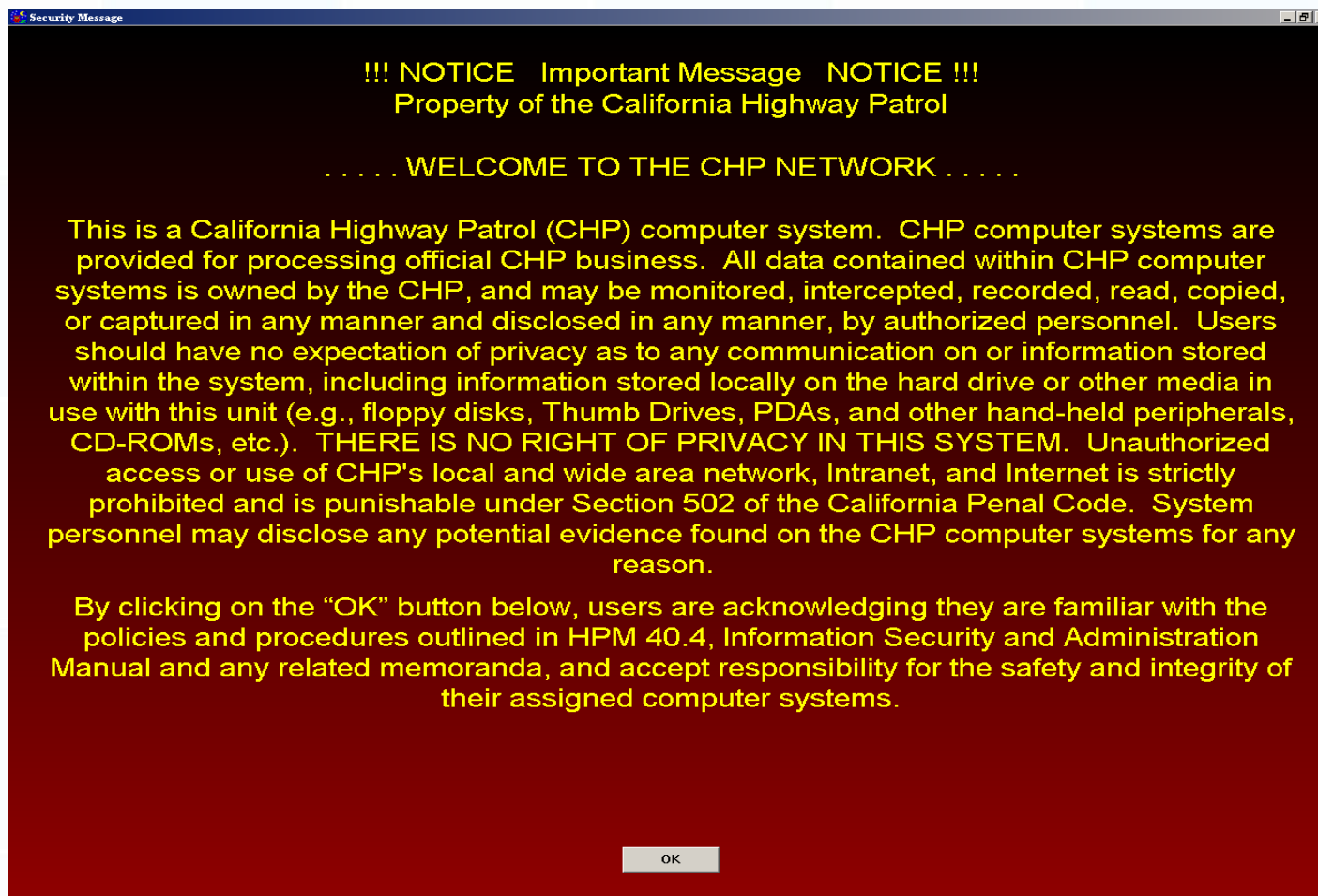
Observations/Trends



- Malware
- Social Engineering and Phishing
- Copyright Infringement
- Compromised credentials
 - Employee/Remote user accounts


California Highway Patrol Computer Crimes Investigations Unit

Banner



Appropriate Use Statement

STATE OF CALIFORNIA
DEPARTMENT OF CALIFORNIA HIGHWAY PATROL
APPROPRIATE USE OF AUTOMATED
INFORMATION & SYSTEMS STATEMENT
 CHP 100 (Rev. 6/27) CH 141



I understand that I may have access to confidential information from any Department of California Highway Patrol (CHP) computer system under the California Law Enforcement Telecommunications System (CLETS). Confidential information includes criminal history, Department of Motor Vehicles (DMV) personnel, and other sensitive records.

I understand that release of information in automated records is a violation of the law and could adversely affect the civil rights of the individual whose records are released.

I understand that Mobile Digital Computer (MDC) transmissions and files can be accessed under the California Public Records Act (Government Code (GC) Sections 54957-54960). Improper use of any CHP computer system, including MDCs, may expose the Department and myself to unnecessary and unfair and public criticism. In addition, I shall adhere to the laws governing dissemination of information in the workplace including MDCs on any other CHP computer system.

I understand that any employee who releases automated information is subject to criminal prosecution, civil action, and departmental adverse action, including dismissal.

I agree to use all reasonable precautions to ensure that CHP automated information is not disclosed to unauthorized persons or used in an unauthorized manner.

I understand that release of automated information is controlled by the following policies:

Penal Code (PC) Section 832 provides the penalties relating to computer crimes. Misdemeanor violations may be punishable by a fine of up to \$1,000 and one year in jail. Penalties may be punishable by a fine of up to \$10,000 and three years in prison. PC Sections 11108 and 10088 identify violations in criminal history information and under other circumstances it may be released. PC Sections 11145.11044 and 10081.11058 provide penalties for release of criminal history information. GC Section 8326 provides the felony penalties for release of public records and CLETS information.

Also, PC Sections 11102 and 10080 state, "Any person authorized by law to receive a record or information obtained from a record information technology facilities that related to information is a person not authorized by law to receive the record or information is guilty of a misdemeanor."

Government Code Section 18550 states in part, "This System (CLETS) shall be used exclusively for the official business of the state and the official business of any city, county, city and county, or other public agency." Any use of the system for functions other than conducting the business of the State of California is a violation of this Section. This includes using the system for private, personal or other non-business purposes.

California Vehicle Code Section 1801.40 prohibits release of CHV record information. Penalties include a fine not to exceed \$5,000 or one year imprisonment in the county jail.

I understand that CHP computing, networking and automated information resources shall not be used for private or personal purposes. I agree to use these resources only for the business of the State of California. This includes business with the federal government and any city, county or other public agency.

I understand that United States and International Copyright Laws protect software, and that copying or reproducing any part of software is a federal crime, except as outlined in a Software License Agreement. I agree to abide by the terms of Software License Agreements.

I understand that before I copy, store, or transfer files on removable media (disettes, CDs, DVDs, thumb drives, external hard drives, flash memory, flash drives, and any similarly functioning device), I must scan the files for computer viruses. In addition, I understand that I must scan the files I receive from Internet sources for computer viruses before I print the files or a CHP network server, or transfer the files to others.

I acknowledge users have no expectation of privacy when using state or non-state owned electronic devices (portable media, cameras, PDAs, laptops, cell phones, and accessories) are connected to the CHP network.

I have read the information in this statement.

I understand the policies, terms, and penalties regarding the release of CLETS and computer-generated information, including criminal history, CHV, and other confidential automated records. I understand the policies and penalties regarding release of CHP computer systems, CHP resources, and Software License Agreements. I understand this failure to abide by these policies and laws may result in disciplinary action or a civil lawsuit. I understand that signing this agreement is a condition of employment as CHP.

State is employee's field personnel before the statement relating:

<p>_____ <small>Signature of field personnel</small></p>	<p>_____ <small>Signature</small></p>
<p>_____ <small>Signature of supervisor</small></p>	<p>_____ <small>Signature</small></p>
<p>_____ <small>Signature of supervisor</small></p>	<p>_____ <small>Signature</small></p>
<p>_____ <small>Signature of supervisor</small></p>	<p>_____ <small>Signature</small></p>

Revised previous edition.

CHP 100 6/27

Questions